UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,618	02/16/2006	Jovan Golic	09952.0025	9355

22852 7590 06/07/2010
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
SHOLEMAN, ABU S

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/07/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/568,618	GOLIC, JOVAN	
	Examiner	**Art Unit**	
	ABU SHOLEMAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-82* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 February 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

Response to Amendment

1. This action is in response to the request for re-consideration filed on 03/09/2010.

2. Claims 42, 46-48, 50-52, 57, 63-67, 69 and 77 have been amended.

3. Applicant's arguments, see pages 12-17, filed on 03/09/2010, with respect to the rejection(s) of claim(s) 42-82 under 35 U.S.C § 103(a) have been fully considered but are moot in view of the new ground(s) of rejection is made.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 42- 82are rejected under 35 U.S.C. 102(e) as being anticipated by Lim (US 20020012430) (hereinafter Lim).

As per claim 42, Lim discloses "A combinatorial key-dependent network for encryption / decryption of input digital data (par 0030, 64 bit input data) having a first word size into output digital data of the same word size (par 0030, 64 bit cipher text output), comprising at least two layers (par 0030, 8 input buffer), each layer comprising at least an elementary building block, each building block operating on an input block of bits having a second word size (Fig.6, 32 bit (IBR(L) 610) equal to said first word size (Fig .6, 32 bit (IBR) 620) for generating an output block of bits, said building block comprising:

"a multiplexer circuit (par 0065 multiplexer 750) , that receives a first portion of said input block of bits and a first set of key bits as inputs (par 0056, and Fig .6, the time multiplexed cipher function receives 32 bits from IBR 620 [first portion] and Kb [first set of key] at Fb), the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit (Fig .6, Fb outputs 32 bits key bits [second set of key] , said first portion of bits are transferred intact to an output of said building block (Fig.6, 32 bits from IBR 620 to transferred into OBR 650) and the number of bits in the second set of key bits is less than the number of bits in the first set of key bits (Fig. 6 output of fb is 32 bits [second set of key] that is less than the Kb 48 bits [first set of key] at kb); and

a transformation circuit (Fig. 6, numeral 632 XOR), for transforming a second portion of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected second set of key bits (Fig .6, input of numeral 632 are 32 bits [second portion] and 32 bits from fb [second set of key bits], among a plurality of reversible transformations implemented in said transformation circuit (Fig.1, DES, each block with XORed [reversible transformations]). wherein said transformation circuit transforms said remaining second portion of said input block of bits without receiving said first portion of said input block of bits as an input (Fig.6, numeral 632 Xored 32 bits from IBRL (second portion) and 32 bits from fb. it does not receive 32 bits from IBR (r) 620 [first portion]) and said output block of bits comprises the transformed bits followed by said first portion of said input block of bits (Fig.6, numeral 632 outputs 32bits to the OBRL and IBR 620 [first portion] outputs to the OBR 650).

As per claim 43, Lim discloses "wherein adjacent layers are connected by means of a fixed bit permutation block" as (Fig, 7, numeral 760, 48 bit [fixed bit] permutation unit).

As per claim 44, Lim discloses "comprising a plurality of fixed bit permutation blocks of the same type" as (Fig.7 , numeral 760 for every block in DES).

As per claim 45, Lim discloses "comprising at least two different types of fixed bit permutation blocks" as (Fig.7, numeral 760 for 48 bits permutation unit and numeral 770 for 32 bits permutation unit).

As per claim 46, Lim discloses "wherein bits in said first portion of said input block of bits are used, in a next layer, as bits to be transformed" as (Fig.6, par 0058, 8 bits data block 610 is output to the 650 for next layer in DES).

As per claim 47, Lim discloses “wherein, for each building block, said first portion of said input block of bits are extracted from at least two building blocks in a preceding layer, provided that said first portion of said block of bits comprise at least two bits (Fig.6, par 0058, block 610 [first portion of block] is 8 bits that is at least 2 bits).

As per claim 48, Lim discloses “ wherein , for each building block, said second portion of said input block of bits are extracted from a least two building blocks in a preceding layer, provided that said second portion of said block of bits comprises at least two bits(Fig.6, par 0058, block 620 [second portion of block] is 8 bits that is at least 2 bits).

As per claim 49, Lim discloses “wherein each layer comprises at least two building blocks” as (Fig.6, layer consists of two blocks IBR (L) 610 and IBR (R) 620).

As per claim 50, Lim discloses “wherein said reversible transformations are such that each output bit of said transformed bits is a non-linear function of said first portion of said input block of bits and of said second set of key bits, with the algebraic normal form containing at least one binary product involving both second portion of said input block of bits and said second set of key bits (Fig.6, numeral 632 XORed 32 bits of 610 [second portion] and 32 bits [second set of key bits] from the Multiplexed).

As per claim 51, Lim discloses “wherein said reversible transformation satisfy a criterion that the uncertainty of the second portion of said input block of bits provided by uniformly random second set of key bits when the transformed bits are known is equal to a bit size of the transformed bits (Fig.6, numeral 632 XORed 32 bits of 610 [second portion] and 32 bits [second set of key bits] from the Multiplexed and output of the numeral 632 is equal to the transformed 32 bits from the transformed bit 32 of numeral 610).

As per claim 52, Lim discloses “wherein said multiplexer circuit comprises as lookup table whose content is defined by the first set of key bits (Fig.7, numeral 750 includes S-box [lookup table]).

As per claim 53, Lim discloses “wherein said transformation circuit comprises XOR gates and controlled switches (Fig.7, and par 0063, XOR and numeral 632 [control switch]).

As per claim 54, Lim discloses " wherein each XOR gate has two input bits and one output bit. one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit" as (Fig.7, par 0063 XOR and control signal).

As per claim 55, Lim discloses “wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch" as (Fig.7, par 0063, XOR and control signal).

As per claim 56, Lim discloses “ wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch" as (Fig.7, par 0063, XOR and control signal).

As per claim 57, Lim discloses “ wherein a second input bit of each XOR gate is connected to a bit of said second portion of said block of bits” as (Fig.6, 32 bits [second portion] is from IBR numeral 610 input 32 bits).

.

As per claim 58, Lim discloses “ wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch" as (Fig.6, output 32 bits from numeral 632 are connected with two inputs 32 bits from numeral 610 and 32 bits from multiplexed circuit fb).

As per claim 59, Lim discloses “wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit" as(Fig.6, numeral 632 [controlled switch] generates transformed bits).

As per claim 60, Lim discloses “comprising a plurality of building blocks of the same type" as (Fig .6, input byte stream are the same).

As per claim 61, Lim discloses “comprising at least two different types of building blocks” as (Fig.6, input stream and output stream. there are two different streams).

As per claim 62, Lim discloses "wherein adjacent layers are connected by means of a block implementing a reversible liner function" as (Fig. 6, each block with an Xored of numeral 632 [reversible linear function]).

As per claim 63, Lim discloses “ wherein two additional input and output keys having word size equal to the first word size are bitwise XORed respectively with said input digital data and with said output digital data (Fig.6, numeral 632 xored the input bits 32 and key bits from the fb).

As per claim 64, Lim discloses" wherein said first set of key bits in each layer, having a first bit size, are generated from a smaller number of secret key bits, having second bit size, by means of a key expansion algorithm (Fig.6, and Fig.7, each layer has a Kb that is 48 bits and used expansion permutation 710).

As per claim 65, Lim discloses “wherein said k secret key bits are first expanded by means of liner transformation into said first set of key bits, using a linear code so that any subset of expanded key bits having a third bit size, are linearly independent ,where the third bit size is less than or equal to the second bit size (Fig.7, Fb transformed the first key kb into second key 32 bits using fb in the multiplexer).

As per claim 66, Lim discloses “ wherein said expanded key having first bit size is used as an input to a further combinatorial key-dependent network having a of block size equal to the first bit size which is parameterized by a fixed randomly generated key satisfying the condition that every multiplexer implements balanced binary lookup tables” as (Fig.7, numeral 710 is the key expansion).

As per claim 67, Lim discloses “ wherein the expanded key having the first bit size produced after every two layers of said further combinatorial key-dependent network are used as said first set of key bits from the multiplexer circuits within the layers of the combinatorial network" as (Fig.6, each layer used kb [first key set] in DES).

As per claim 68, Lim discloses “a multiplexer having one input receiving one control bit which is passed to the output intact, for selecting one out of two key bits on a one bit output and a controlled switch having two input bits, two output bits and one control bit connected to the output of said multiplexer, said control bit determining if said two input bits are swapped or not" as(Fig.6, and Fig. 7, numeral 750 [multiplexer] used for selecting bits from two inputs).

As per claim 69, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 70, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 53 above, and accordingly is rejected for similar reasons.

As per claim 71, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 54 above, and accordingly is rejected for similar reasons.

As per claim 72, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 55 above, and accordingly is rejected for similar reasons.

As per claim 73, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 56 above, and accordingly is rejected for similar reasons.

As per claim 74, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 57 above, and accordingly is rejected for similar reasons.

As per claim 75, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 58 above, and accordingly is rejected for similar reasons.

As per claim 76, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 59 above, and accordingly is rejected for similar reasons.

As per claim 77, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 78, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 43 above, and accordingly is rejected for similar reasons.

As per claim 79, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 44 above, and accordingly is rejected for similar reasons.

As per claim 80, this claim is directed to a block for secret-key controlled cryptographic functions and contains limitations that are substantially similar to those recited in claim 50 above, and accordingly is rejected for similar reasons.

As per claim 81, this claim is directed to a data processing device and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 82, this claim is directed to a multimedia device and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

Examiner Notes

6. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314 and Fax number is (571)-270-8314. The examiner can normally be reached on Monday through Thursday 9:30 AM - 6:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABU SHOLEMAN/

Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437